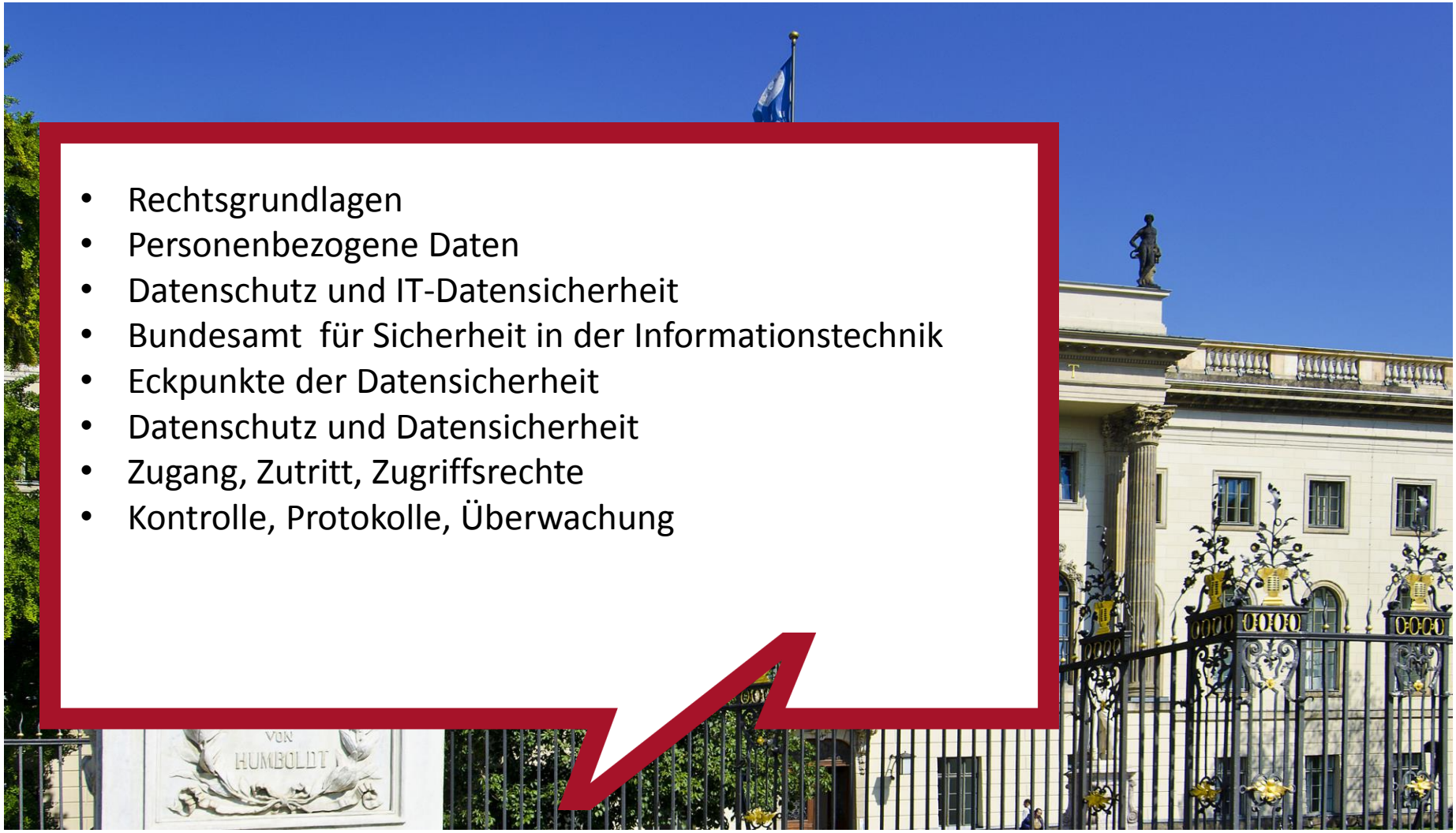
Datenschutz und Datensicherheit in Schulverwaltungssystemen

Fachtagung „Datenschutz in der mediatisierten Schule, 23. und 24. Oktober 2014“

Kay Hansen



- Rechtsgrundlagen
- Personenbezogene Daten
- Datenschutz und IT-Datensicherheit
- Bundesamt für Sicherheit in der Informationstechnik
- Eckpunkte der Datensicherheit
- Datenschutz und Datensicherheit
- Zugang, Zutritt, Zugriffsrechte
- Kontrolle, Protokolle, Überwachung

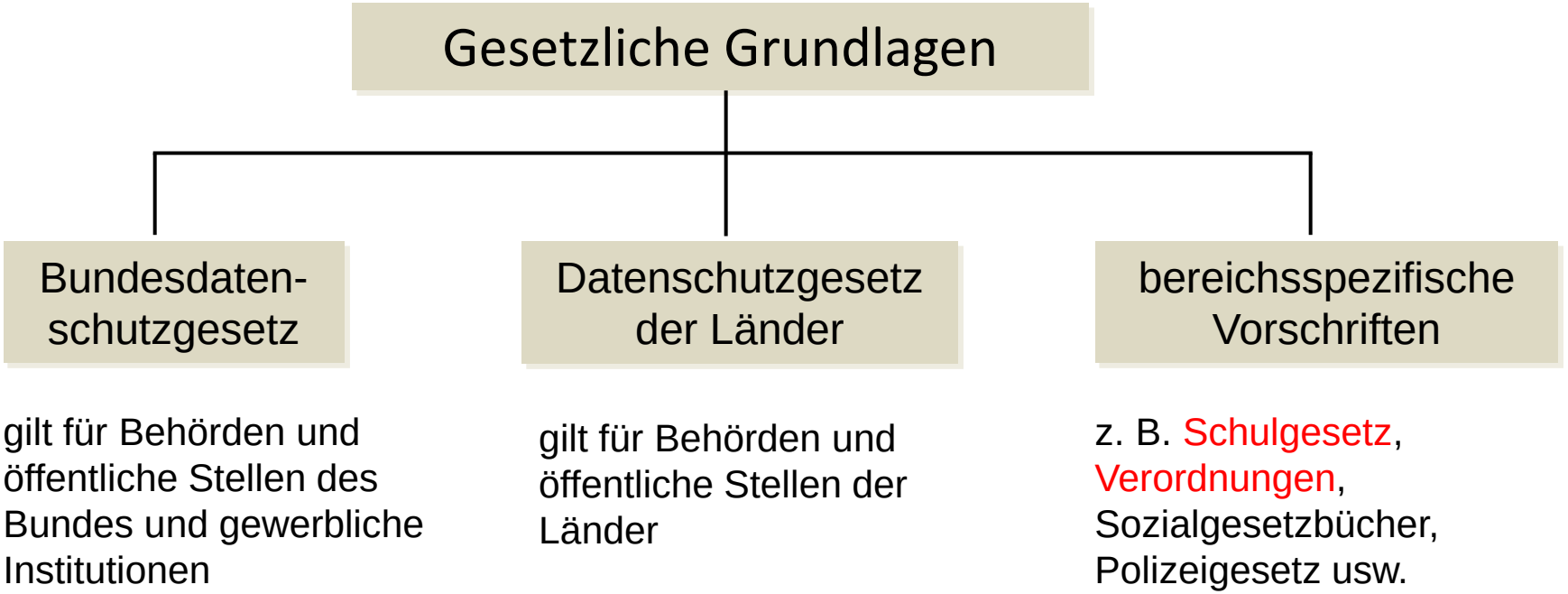
Die grundsätzlichen Rechtsgrundlagen für den Datenschutz lassen sich u. a. ableiten.

- **Grundgesetz**
  - Artikel I
    (1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.
    Artikel II
    (1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

- **Bundesdatenschutzgesetz**
  - § 3a Datenvermeidung und Datensparsamkeit
    Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

- **Volkszählungsurteil vom 15.12.1983**
  - Das Recht auf informationelle Selbstbestimmung ist das Recht jedes Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Quelle: *www.bfdi.bund.de*

Rechtsgrundlagen für die Schulverwaltung.



Verantwortung für die Einhaltung der rechtlichen Regelungen: **Schulleitung**

Personenbezogene Daten sind Einzelangaben über:

- **Persönliche Umstände**
  - Z. B. Name, Anschrift, Familienstand, Geburtsdatum, Beruf, Fingerabdruck, persönliche Überzeugung, Bankverbindung, Beruf, Fotos.

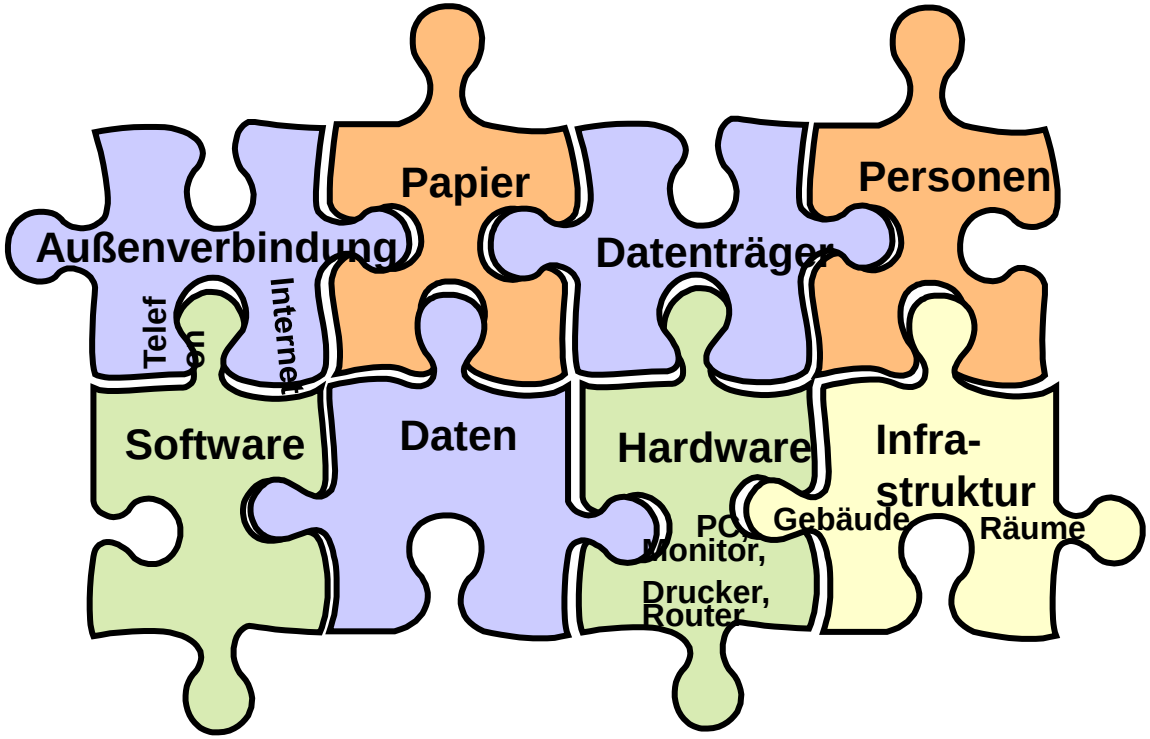
- **Sachliche Verhältnisse der Person**
  - Z. B. über Eigentumsverhältnisse, vertragliche Beziehungen und Verbindungen, Konsumverhalten, Kommunikationsverhalten.

- **Bestimmbarkeit (Identifikation) einer Person**
  - Bestimmbar ist eine Person, wenn sie nicht über vorhandene Daten allein, jedoch mit Hilfe weiterer Merkmale identifiziert werden kann.
  - Dies gilt für natürliche Personen – nicht für juristische Personen.

- **Art der Erfassung und Darstellung**
  - Dies gilt unabhängig von der Art der Erfassung, Technik und der Darstellung (wie z. B. Bilder, Texte, analoge oder digitale Verarbeitung).

Wenn personenbezogene Daten mit Hilfe von Informationstechnologie verwaltet werden, ist die Frage der IT-Sicherheit mit zu beachten:

- **IT-Sicherheit betrifft jeden, der mit Informationstechnologien arbeitet.**
- **IT-Sicherheit funktioniert am wirkungsvollsten, wenn in allen Bereichen und von allen Beteiligten ein verantwortungsvolles abgestimmtes Verhalten erfolgt.**



Grundlagen, Fragen, Hinweise, Hilfen zur Erhaltung von Datenschutz und Datensicherheit - das BSI hilft.

- **Angesichts der vielfältigen und wachsenden Gefährdungspotentiale und der steigenden Abhängigkeit stellen sich damit für alle Anwender hinsichtlich der Informationssicherheit die Fragen, wie kann ich mit welchen Mitteln mehr Sicherheit erreichen**

- **Das BSI stellt zahlreiche Werkzeuge zur Verfügung, um ein angemessenes Sicherheitsniveau zu erreichen, wie z. B. die BSI-Standards zum Informationssicherheitsmanagement, die IT-Grundschutz-Kataloge und das GSTOOL**

- **Dazu gehört aber auch die ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, die sowohl eine Prüfung des Informationssicherheitsmanagements als auch der konkreten Sicherheitsmaßnahmen auf Basis von IT-Grundschutz umfasst**

Die IT-Sicherheit lässt sich mit folgenden Eckpunkten beschreiben

- **Vertraulichkeit**
  - Sensible Daten (z. B. personenbezogen) müssen vertraulich bleiben und dürfen unberechtigten Personen nicht zugänglich sein
- **Integrität**
  - Daten oder Systeme dürfen weder unberechtigt noch zufällig verändert oder gelöscht werden
- **Authentizität**
  - Bei der Anmeldung an einem System, PC oder an einem IT-Verfahren wird die Identität der Person, die sich anmeldet, geprüft (Name und Passwort) und damit deren Berechtigung, auf bestimmte Daten oder Systeme zuzugreifen, nachgewiesen
- **Verfügbarkeit**
  - Die Daten müssen an bestimmten Orten und zu bestimmten Zeiten zuverlässig verfügbar sein

Sicherheitsstörungen können den Datenschutz auf unterschiedliche Art bedrohen: z. B.

- **Unberechtigte Datenmanipulation**
  - Der Zugang zu einem IT-System erfolgt mit falscher Identität und Datensätze werden manipuliert (z.B. Noten)
- **Geplanter „Datenklau“**
  - Daten werden aus dem System unberechtigt abgezogen und verwendet (z. B. Verkauf)
- **Unbeabsichtigter Datenverlust aufgrund fehlerhafter Anwendung oder defekter Infrastruktur**
  - Elektronisch gespeicherte Daten stehen nicht mehr zur Verfügung, um Sachstand/Leistungsstand/Profil zu belegen
- **Gestörter Zugriff auf die erforderlichen Daten in kritischen Phasen**
  - Erforderliche Zeugnisse können nicht gefertigt werden und verhindern bei den Betroffenen eine fristgerechte Bewerbung
- **Vertrauliche Daten kommen in die „falschen“ Hände**
  - Besonderer Förderbedarf wird bekannt gegeben und verhindert eine Einstellung

Zugangsberechtigungen und Zugriffsrechte müssen geklärt sein.

- **Maßnahmen zur Raum- und Gebäudesicherheit**
  - Es muss gesichert sein, dass der Zutritt zum Gebäude geregelt ist, Ausnahmen (z. B. Elternabende) müssen besonders beachtet werden

- **Zugang zu Räumen mit IT-Infrastruktur**
  - Ausschließlich autorisierte Personen haben Zugang (dokumentierte Schlüsselvergabe)
  - Unberechtigte Personen (z. B. Schüler) haben nur beaufsichtigten Zugang (Ausnahmen, z. B. für Reinigungspersonal, Wartung der Geräte etc. müssen gesondert geregelt werden)
  - Bei Abwesenheit sind diese Räume (Fenster und Türen) verschlossen zu halten

- **Anmeldung an das System**
  - Zur Authentifizierung erhält jeder zur Anmeldung an das System einen Benutzernamen mit Passwort
  - Das Passwort muss nach dem ersten Login gewechselt werden
  - Das Passwort muss vorgegebenen Regeln entsprechen
  - Für das Passwort muss es ein Ablaufdatum geben

- **Aufgabenbezogene Zugriffsberechtigungen innerhalb der Anwendung**
  - Trennung von Lese- Schreib- und Löschrechten
  - Administrator dient ausschließlich der Nutzereinrichtung und Zuweisung von Rechten
  - Ein Rollen- und Rechtekonzept regelt die aufgabenbezogenen Zugriffsberechtigungen der Nutzer
  - Die Schulleitung legt die Zuweisung der Rollen und Personen fest

(Programm)Technische Vorkehrungen müssen die Einhaltung der IT-Sicherheit kontrollieren, protokollieren und überwachen.

- **Protokollierung und Meldung zum Anmeldeverhalten**
  - Welche User wurden mit welchen Rechten zu welchem Zeitpunkt eingerichtet
  - Es wird angezeigt, wenn sich der User ordnungsgemäß (Abmeldefunktion) abmeldet
  - Zugangsberechtigungen sollten bei länger währender Abwesenheit einer berechtigten Person vorübergehend gesperrt werden

- **Protokollierung von Datenbankaktionen (schreiben, lesen, löschen)**
  - Welche Daten wurden von welchem User zuletzt verändert oder gelesen
  - Sind (eventabhängig) auffällige Datenbankaktionen zu verzeichnen (penetrante Anmeldeversuche, unverhältnismäßige Löschvorgänge)
  - Die Kontrolle der durchgängigen Protokollierung muss erfolgen (wie ist es bei Updates mit Systemneustart geregelt)
  - Wer hat Zugriff auf die Protokolle und darf Auswertungen vornehmen

- **Reaktion bei Auffälligkeiten unterscheiden sich nach der Sicherheitsrelevanz**
  - Bei sicherheitsrelevanten Vorkommnissen (Änderungen von Passwörtern, Anwenderrollen wurden verändert, Benutzer wurden gelöscht) muss eine automatische Information ausgelöst werden
  - Datenveränderungen ohne unmittelbare Sicherheitsrelevanz werden für gezielte Analysen protokolliert (z. B. Änderungen von Leistungsdaten, Stammdaten, usw.)